REMARKS

Applicants appreciate the Examiner's thorough review of the present application, and respectfully request reconsideration in light of the preceding amendments and the following remarks.

Claims 1-25 are pending in the application. Several original claims have been amended to better define the claimed invention. New claims 23-25 have been added to provide Applicants with the scope of protection to which they are believed entitled. The amended/new claims find solid support in the original specification, e.g., at page 9, lines 12-13, page 10, lines 7-11 and 17-18, page 11, lines 8-9, and the drawings. The Abstract has been revised to comply with commonly accepted US patent practice. No new matter has been introduced through the foregoing amendments.

The *35 U.S.C. 112, second paragraph* rejections are noted. Although Applicants do not agree with the Examiner's position that the original claims are indefinite, claim amendments have nevertheless been made to avoid the rejections, solely for the purpose of expediting prosecution. In particular, independent claims 1 and 15 have been amended to change "the configuration" to --a configuration--. Further, in independent claim 15, "being arranged to" has been changed to --adapted to-- as commonly accepted in US patent practice. Withdrawal of the rejections is now believed appropriate and therefore respectfully requested.

The *35 U.S.C. 102(b)* rejection of claims 1-22 as being anticipated by *Chaiken* (EP 1 072 975) is traversed, because the reference, as applied by the Examiner, does not fairly teach or disclose each and every element of the rejected claims.

For example, as to independent claim 1, the reference, as applied by the Examiner, does not fairly teach or disclose "a non-volatile storage medium including configuration data that describes a configuration of the non-volatile storage medium." The Examiner's reading of the *Chaiken* BIOS stored on ROM 102 on the claimed configuration data and non-volatile storage medium, respectively, is noted.[1] Applicants respectfully disagree with the Examiner's interpretation of the reference, because the *Chaiken* BIOS is not disclosed to describe a configuration of ROM 102. Rather, the BIOS as taught by *Chaiken* is

> "a piece of code that the PC 100 uses to get itself started when the computer is switched on. In some cases, the BIOS is further utilized to manage data transactions between hardware and programs. Hardware that is "set up" by the BIOS may include RAM memory 106, hard or floppy disk drives 108, input/output circuitry 110, and modem circuitry 112."[2]

A person of ordinary skill in the art would understand that a BIOS generally does not describe a configuration of the ROM in which the BIOS resides. The person of ordinary skill in the art would also recognize from the above reproduced teaching of *Chaiken* that the reference's BIOS only includes, if at all, configuration data of the components set up by the BIOS, such as RAM memory 106, hard or floppy disk drives 108, input/output circuitry 110, and modem circuitry 112. Since ROM 102 is not disclosed to be configurable by the BIOS, no configuration data of ROM 102 is required to be included in the BIOS.

The reference, as applied by the Examiner, apparently fails to teach or disclose at least the above-discussed limitation of independent claim 1, and therefore fails to anticipate claim 1.

[1] *See*, for example, Office Action at page 3, line 3.

[2] *See*, for example, *Chaiken* at column 3 lines 27-34.

Independent claims 15 and 16 also include the above-discussed limitation of independent claim 1, and are believed patentable over the applied reference for at least the same reason advanced with respect to independent claim 1.

The dependent claims are considered patentable at least for the reasons advanced with respect to the respective independent claims. The dependent claims are also patentable on their own merits since these claims recite other features neither disclosed, taught nor suggested by the applied art, as will be apparent to the Examiner upon reviewing these claims.

For example, as to claims 4 and 6, Applicants respectfully disagree with the Examiner's allegation that paragraphs 0014 and 0016 of *Chaiken* teach the claimed Master Boot Record or Master Boot Code. The terms have well-recognized definitions in the art which are not deemed met by any teaching found in the Examiner's cited passages.

As to claim 8, the Examiner's cited paragraphs 0020-0022 of *Chaiken* do not appear to fairly teach or disclose that the decrypter is arranged to decrypt the configuration data in response to a determination that the first software is authorized to access the configuration data. Thus, claimed 8 requires that the configuration data be decrypted *after* the determination that the first software is authorized to access the configuration data. The cited portions of *Chaiken*, however, teach how decryption of the "configuration data," i.e., BIOS image, can be used to make such determination. In other words, the cited portions of *Chaiken* teach that decryption occurs *before or at the same time* as the determination, and hence, do not read on the claim language. In addition, it should be noted that, in *Chaiken*, in response to "a determination that the first software is authorized to access the configuration data" (i.e., the new BIOS is certified, box 218, Fig. 2), there will be *no decryption* of the "configuration data" or BIOS. Instead, the "configuration data" or BIOS will be flashed or *replaced* with a new version (boxes 220-222, Fig. 2). Thus, claim 8 is not anticipated by *Chaiken* as applied by the Examiner.

As to claim 13, the Examiner's cited Fig. 3 of *Chaiken* does not appear to fairly teach or disclose an operating system stored in the non-volatile storage medium. The OS 304 in Fig. 3 of *Chaiken* is not disclosed to be stored in the "non-volatile storage medium" or ROM 102.

As to claim 23, *Chaiken* as applied by the Examiner does not fairly teach or disclose that the uninterruptible software routine has code for hanging the data processing system in response to a determination that the first software is not authorized to access the configuration data. In *Chaiken*, if BIOS flash is not authorized, the system will not hang.[3]

As to claim 24, *Chaiken* as applied by the Examiner does not fairly teach or disclose that the controller is an I/O controller hub. The "controller" in *Chaiken* as applied by the Examiner is the BIOS flash utility.[4]

As to claim 25, *Chaiken* as applied by the Examiner does not fairly teach or disclose generating and sending an SMI interrupt to the processor in response to any attempt by the first software executing within the first mode of operation of the processor to access the configuration data. In *Chaiken* as applied by the Examiner, an SMI interrupt is generated only after the CPU has approved the BIOS flash request as intentional.[5]

[3] *See*, for example, *Chaiken* at column 6 line 36.

[4] *See*, for example, *Chaiken* at paragraph 0028.

[5] *See*, for example, *Chaiken* at column 7 lines 33-37.

Each of the Examiner's rejections has been traversed. Accordingly, Applicants respectfully submit that all claims are now in condition for allowance. Early and favorable indication of allowance is courteously solicited.

The Examiner is invited to telephone the undersigned, Applicant's attorney of record, to facilitate advancement of the present application.

To the extent necessary, a petition for an extension of time under 37 C.F.R. 1.136 is hereby made. Please charge any shortage in fees due in connection with the filing of this paper, including extension of time fees, to Deposit Account 08-2025 and please credit any excess fees to such deposit account.

Respectfully submitted,
Paul NEUMAN *et al.*

Benjamin J. Hauptman
Registration No. 29,310

HEWLETT-PACKARD COMPANY
Intellectual Property Administration
P.O. Box 272400
Fort Collins, CO 80527-2400
Telephone: 703-684-1111
Facsimile: 970-898-0640
Date: June 5, 2007
BJH:KL/tal